explicit recitation" of the claimed subject matter, but concluded that "[i]t would have been obvious to a person of ordinary skill in the art at the time of the invention that the disclosure of Killian ... would have been selected in accordance with [claimed subject matter] because such selection would have provided means for 'secure electronic, voting ... to enable secret votes to be performed electronically where the votes of individual voters are unknown and where the votes of individual votes are unknown and where the election results are tamper-proof" (the Examiner cited Killian at col. 2, lines 39-45).

The portion of Killian cited by the Examiner reads as follows:

> The idea of secure electronic, voting is to enable secret votes to be performed electronically where the votes of individual voters are unknown and where the election results are tamper-proof without the collusion of many counting centers. The present invention relies upon a novel mathematical method to encode votes for verification by breaking up the vote into shares which are supplied to different counting centers.

In response to the Examiner's assertions of obviousness, applicants assert that Killian, as discussed above cannot be found to disclose or even suggest the subject matter of the present invention. As quoted above, Killian addresses issues of privacy in electronic voting by splitting a single vote into a number of separate "shares", as discussed throughout the remainder of Killian, where different counting centers process each share, such that the shares are ultimately re-combined to form the single vote.

In complete contrast, the subject matter of the present invention is directed to setting up secure voting scheme wherein a voter first sets up a voter registration in terms of voting authorization data that is atomically bound to a blinded unvalidated vote certification to be validated (claim 1). The voting center then validates the blinded vote certificate and returns it to the voter. Thereafter, the voter submits an unblinded vote certificate and a blinded unvalidated vote certificate to be validated (claim 5). There is no discussion of atomically binding any two pieces of information in Killian, let alone utilizing both an unblinded vote certificate and a blinded unvalidated vote certificate.

In general, the subject matter of the present invention relies on the atomically bound relationship between unblinded certificates and blinded, unvalidated vote certificates to allow for anonymity in the voting process. Killian relies on splitting a single vote into a number of different shares to allow for anonymity. These are

considered to be patentability distinct arrangements. Moreover, the subject of providing an "audit" by the voting center (claims 11, 12, 23, 25) is not even suggested by Killian.

Based upon these significant differences between the subject matter of Killian and the subject matter of the present invention as defined by claims 1-27, applicants respectfully request the Examiner to reconsider the rejections and find all claims 1-27 to be in condition for allowance. If for some reason or other the Examiner does not agree that the case is ready to issue and that an interview or telephone conversation would further the prosecution, the Examiner is invited to contact applicants' attorney at the telephone number listed below.

Respectfully submitted,

David M. Goldschlag
Stuart G. Stubblebine
Paul F. Syverson

By: Wendy W. Koba
Wendy W. Koba
Reg. No. 30509
Attorney for applicants
610-346-7112

Date: 2/20/03

Bracketed and Underlined Specification Amendments for App. 09/635,778

Please **amend** the paragraph beginning at **line 25 of page 14** to read as follows:

--An embodiment of the redemption process in accordance with the present invention is shown in FIG. 2. A first party (e.g., a [customer] voter) unblinds a validated blinded vote certificate, step 201. The blinded validated vote certificate was validated either by a registrar as the result of a successful registration (see FIG. 1, step 103), or by a second party (e.g., a [vendor] voting center) as the result of a successful earlier redemption. A transaction request message is received at the [second party] voting center from a registered first party (e.g., a registered [customer] voter), step 202. The transaction request message atomically binds an unblinded vote certificate with a blinded unvalidated vote certificate to be validated. In one embodiment of the present invention, the blinded unvalidated vote certificate is a blinded hashed nonce. The [second party] voting center determines if the unblinded vote certificate is valid, step 203. If the unblinded vote certificate is valid, then a transaction response is performed, step 204.--

Please **amend** the paragraph beginning at **line 22 of page 15** to read as follows:

--In Message 1, a validated unblinded hashed none h(Ni) is sent with the nonce, Ni and the key Kcv are sent confidentially from the customer C (the voter) to the vendor (the voting center). Also sent is an authenticated request for a transaction of type S and an unvalidated blinded hashed (new) nonce, h(N(i+1)). The [vendor] voting center performs the one-way hash function on nonce Ni and compares the result to the validated unblinded hashed nonce h(Ni). If the two correspond, then the [vendor] voting center determines that the validated unblinded hashed nonce is a valid vote certificate, sends an approval message in Message 2, and engages in the transaction of Message 3. Finally, the [vendor] voting center validates the blinded hashed nonce of Message 1 and sends it to the [customer] voter. In one embodiment, the [customer] voter then sends an authenticated acknowledgment message upon receiving the validated blinded hashed nonce from the[vendor] voting center:

Message 5: C->V: [Ack]Kcv.--

Please **amend** the paragraph beginning at **line 12 of page 16** to read as follows:

--In one embodiment of the present invention, a transaction response includes validating the blinded unvalidated vote certificate to obtain a validated blinded vote certificate, and sending the validated blinded vote certificate atomically bound to the transaction request message to a transaction response recipient. [A transaction response recipient can be the first party (e.g., customer) or another party. For example, in one embodiment, a transaction response is a gift sent to a third party. In another embodiment, a transaction response message is a control signal sent to a piece of factory equipment. In one embodiment, the present invention provides a way for anonymous monitoring of a piece of equipment. When the status of the equipment is desired by an authorized (i.e., registered) entity, the entity sends an unblinded validated certificate and blinded unvalidated certificate to the equipment, which sends back status data along with a validated blinded certificate in accordance with the present invention]--

Please **delete** the paragraph beginning at **line 3 of page 17.**

Please **amend** the paragraph beginning at **line 12 of page 17** to read as follows:

--In one embodiment of the present invention, audit data is included to help protect against fraud. The transaction request message atomically binds an unblinded vote certificate, a blinded unvalidated vote certificate to be validated, and blinded audit data. Not every message is audited, so the blinding of the audit data protects the privacy of the [first party] voter when no audit is performed.--

Please **amend** the paragraph beginning at **line 19 of page 17** to read as follows:

--Audits are typically performed randomly in accordance with the present invention. However, audits can also be triggered, for example, by unusual service activity that may indicate that a [subscriber] voter is sharing its vote certificates with others[, non-paying parties. For example, an exceptionally high volume of traffic accessing a database or telephone service may indicate a heightened necessity for audits of transaction requests accessing the database or service.]--

Please **amend** the paragraph beginning at **line 28 of page 17** to read as follows:

--An embodiment of the audit method in accordance with the present invention is shown in FIG. 3. During registration, the [customer] voter provides an audit secret to the [registrar] voting center. [In this embodiment, the registrar is also the vendor. In another embodiment, the registrar is a third party.] During the redemption process, every transaction request message from the [customer] voter includes a blinded version of the audit secret. Thus, the [vendor] voting center receives a transaction request message with a blinded audit secret, step 302. Rather than sending an audit response message to the [customer] voter, the [vendor] voting center sends an audit request message atomically bound to the transaction request message, step 303. The [vendor] voting center receives an audit response message from the customer that includes audit response data, step 304. In one embodiment, the audit response data includes an audit secret and the audit blinding factor. As with the blinded vote certificate, the audit blinding factor is combined with the audit secret in transaction requests to hide the audit secrete from the [vendor] voting center until an audit is initiated by the [vendor] voting center. The [vendor] voting center determines if the transaction request message of step 302 is legitimate using the audit response data, step 305. In one embodiment, the transaction request message is legitimate if the audit secret combined with the blinding factor provided in the audit response message corresponds to the blinded audit secret received in the transaction request message of step 302. If the transaction message of step 302 is determined to be legitimate, step 306, then the [vendor] voting center validates the blinded unvalidated vote certificate received from the [customer] voter in the transaction request message of step 302, step 307. The [vendor] voting center then sends the validated blinded vote certificate to the [customer] voter, step 308. If the transaction request message of step 302 is determined not to be legitimate, step 306, then in one embodiment, the [customer's] voter's transaction is terminated, step 309. That is, no certificate is validated and returned to the [customer] voter.--

Please **amend** the paragraph beginning at **line 3 of page 20** to read as follows:

--Message 1 is a transaction request with audit features. In message 2, the [vendor] voting center V initiates an audit by sending an authenticated audit initiation

message. The [customer] voter sends an audit response message to the [vendor] voting center. The audit response message in this embodiment includes audit data comprising the [customer] voter identifier, C, the nonce Ni, an audit secret Audit_Secret, and Salt. The [vendor] voting center in this embodiment is also the registrar, and so has the Audit_Secret received from [customer] voter C during the registration process. First, the [vendor] voting center compares the audit secret received in Message 3 with the audit secret received from the [customer] voter in the [customer's] voter's registration message. These must correspond in order for the [vendor] voting center to determine that Message 1 is legitimate. The [vendor] voting center also hashes the audit secret, nonce and salt received in Message 3 and compares it to the hashed combination of the audit secret, nonce and Salt received in Message 1. These must also correspond so that the [vendor] voting center knows that the audit secret provided by the [customer] voter in Message 3 is the same as the audit secret embedded in Message 1. If both of these correspondences are established, then the transaction response message (Message 1) is determined to be legitimate, and a validated blinded hash is sent to the [customer] voter in Message 4. In one embodiment of the present invention, an authenticated acknowledgment message is sent from the [customer] voter to the [vendor] voting center when the [customer] voter receives Message 4:

Message 5: C->V: [Ack]Kcv

The purposes of the Salt in the above message is to protect the anonymity of the [customer] voter and the unlinkability of the [customer's] voter's transactions based upon audit information. Without Salt, a [vendor] voting center could associate a transaction request message with a [customer's] voter's identity using h(Ni,Audit_Secret) received in the transaction request message. Recall that when the [vendor] voting center is the registrar, the [vendor] voting center has a record of audit secrets received during the registration process from the [customer] voter, with each audit secret associated with a [customer] voter identifier. A [vendor] voting center could hash the nonce Ni received in a transaction request message with the audit secrets it knows from registration until a match is found with the audit data received in the transaction request message. In order

to prevent such an exhaustive search from revealing a [customer] voter identity, nonce Salt is hashed with the audit secret and nonce Ni in each transaction response message. Because Salt is a nonce, it changes from message to message, rendering the audit data in a transaction request message untraceable by the [vendor] voting center.--

Please **amend** the paragraph beginning at **line 22 of page 21** to read as follows:

--The audit features of the present invention advantageously deter the illicit sharing of voting certificates. An [non-paying] improper party is not likely to have the audit secret, which in one embodiment is a credit card number, or other valuable data for which the registered [customer] voter has a strong incentive to keep confidential. This provides a disincentive for sharing the data that is needed to pass an audit. Illicitly sharing a subscription also incurs a risk of subscription termination, and is thereby further deterred by the present invention.--

Please **amend** the paragraph beginning at **line 3 of page 22** to read as follows:

--The present invention terminates a series of transactions simply by not validating and returning an unvalidated blinded vote certificate as part of the last transaction--.

Please **amend** the paragraph beginning at **line 16 of page 22** to read as follows:

--In one embodiment, broken protocols are considered to be automatically acknowledged after some predetermined period of time, after which the [customer] voter cannot recover from the break, and replay is not allowed. If a connection breaks after the receipt of a new validated blinded vote certificate has been acknowledged by the [customer] voter in the redemption protocol, then the [customer] voter can simply use the new vote certificate in the next transaction request.--

Please **amend** the paragraph beginning at **line 24 of page 22** to read as follows:

--If the connection breaks before the [customer] voter has received the new validated blinded vote certificate in the redemption protocol, then the protocol is replayed. An embodiment of the trusted recovery protocol is shown in FIG. 4. The

[vendor] voting center stores the messages of each protocol run (one instance of Messages 1 through 4 of the redemption protocol above), step 401, until the [vendor] voting center receives an acknowledgment message from the [customer] voter indicating that the [customer] voter has received the new vote certificate (Message 5 in the redemption protocol), or until the predetermined automatic acknowledgment time has elapsed, step 402. When the [customer] voter realizes the connection has been broken, step 403, the [customer] voter replays the protocol run starting from the transaction request message (Message 1 of the redemption protocol), step 404. The [vendor] voting center identifies the presented vote certificate as already spent, and consults its recovery database (in which the protocol runs are stored), step 405. If the recovery database indicates that no acknowledgment from the [customer] voter has been received, step 406, then the [vendor] voting center returns the stored response, step 407. As mentioned above, the transaction is skipped, but the [customer] voter receives a new validated blinded vote certificate to use in the next protocol run to engage in the transaction. Note that the [customer] voter does not identify itself during recovery in accordance with the present invention, advantageously protecting the [customer's] voter's anonymity.--

Please **delete** the paragraph beginning at **line 21 of page 23.**

Please **delete** the paragraph beginning at **line 29 of page 23.**

Please **delete** the paragraph beginning at **line 10 of page 24.**

Please **amend** the paragraph beginning at **line 19 of page 24** to read as follows:

--[Another] In accordance with the preferred embodiment of the present invention, [is used for voting. In this embodiment,] a voter registers and receives a validated, blinded certificate to cast in a vote. The registration process ensures, for example, that each voter is entitled to cast only one vote. In one embodiment, a different electronic destination is provided for each option for which the vote may be cast. The voter unblinds the validated, blinded voting certificate and sends it to the destination corresponding to the option for which the voter chooses to vote. In another embodiment,

the voter indicates its choice in a certificate, blinds it, sends it to be certified, receives it back, unblinds it, and sends it to an electronic destination. For example, in an election with two choices, an even random number (nonce) corresponds to the first choice, and an odd random number (nonce) corresponds to the second choice. The voter picks an odd or even nonce in accordance with the voter's choice, and votes in accordance with the present invention. This advantageously avoids having to designate different destinations for different votes.--

Please **amend** the paragraph beginning at **line 10 of page 25** to read as follows:

--An embodiment of an apparatus in accordance with the present invention is shown in FIG. 5. A server 501 includes a processor 502 coupled to a memory 503 that stores voting transaction instructions 504 that are adapted to be executed on processor 502. Server 501 further comprises a port 505 that is adapted to be coupled to a network 506. Port 505 is coupled to processor 502 and memory 503. A client (e.g., a [customer] voter) 507 is also coupled to the network 506.--

Please **amend** the paragraph beginning at **line 7 of page 26** to read as follows:

--In one embodiment of the present invention, transaction instructions 504 are adapted to be executed by processor 502 to perform the steps of initializing a series of electronic transactions. For example, the instructions are adapted to be executed by processor 502 to receive an initialization request message that atomically binds authorization data and a blinded unvalidated vote certificate to be validated; determine if the authorization data is valid; if the authorization data is valid, then to validate the blinded unvalidated vote certificate to obtain a blinded validated vote certificate; and to send an initialization response message to a registrant that includes the blinded validated vote certificate atomically bound to the initialization request message.--

Please **amend** the paragraph beginning at **line 21 of page 26** to read as follows:

--In another embodiment of the present invention, transaction instructions 504 are adapted to be executed by processor 502 to perform an electronic transaction, e.g., to receive a transaction request message that atomically binds an unblinded vote certificate

and a blinded unvalidated vote certificated to be validated; determine if the unblinded vote certificate is valid; and if the unblinded vote certificate is valid, then to perform a transaction response that validates the blinded unvalidated vote certificate to obtain a validated blinded vote certificate, and sends the validated blinded vote certificate atomically bound to the transaction request message to a transaction response recipient in a transaction response message.--

Please **amend** the paragraph beginning at **line 4 of page 27** to read as follows:

--In yet another embodiment, transaction instructions 504 are adapted to be executed by processor 502 to audit an electronic transaction, e.g., to receive a transaction request message that atomically binds an unblinded vote certificate and a blinded unvalidated vote certificate to be validated and blinded audit data; to send an audit request message atomically bound to the transaction request message to an audit recipient; to receive an audit response message atomically bound to the audit transaction message, where the audit response message includes audit response data; and to determine if the blinded audit data is valid using the audit response data.--

Please **amend** the paragraph beginning at **line 21 of page 27** to read as follows:

--The present invention advantageously provides for anonymous, unlinkable electronic [transactions] voting that assures the [vendor] voting center of [payment] a valid vote being cast while protecting the privacy of the [customer] voter.----